DOCUMENT RESUME

ED 384 307 HE 028 420

TITLE	Federal Family Education Loan Information System. Weak Computer Controls Increase Risk of Unauthorized Access to Sensitive Data. Report to the Secretary of Education.
INSTITUTION	General Accounting Office, Washington, DC. Accounting and Information Management Div.
REPORT NO	GAO/AIMD-95-117
PUB DATE	Jun 95
NOTE	26p.
AVAILABLE FROM	U.S. General Accounting Office, P.O. Box 6015, Gaithersburg, MD 20884-6015 (first copy free; additional copies $2 each; 100 or more copies discounted 25%).
PUB TYPE	Legal/Legislative/Regulatory Materials (090)
EDRS PRICE	MF01/PC02 Plus Postage.
DESCRIPTORS	Access to Information; *Computer Security; Databases; *Federal Programs; Higher Education; *Information Management; *Information Systems; Postsecondary Education; Program Evaluation; *Student Loan Programs
IDENTIFIERS	Data Security; Department of Education; *Family Education Loan Program

ABSTRACT

This report presents an evaluation of the general controls over the Federal Family Education Loan Program (FFELP) information system maintained and operated by a contractor for the U.S. Department of Education (ED), which administers FFELP. The evaluation found that ED's general controls over the FFELP information system did not adequately protect sensitive data files, applications programs, and systems software from unauthorized access, change, or disclosure. ED, for example, did not: (1) adequately monitor the access activities of system users with special privileges that allow them to independently change the system; and (2) record and report and, thus, could not review, successful access to sensitive computer data and programs. Further, outside users could potentially bypass the system's access controls to gain access to the system. The report contains specific recommendations, many of which have already been implemented, to help improve the security of the FFELP information system. Two appendixes contain comments from ED and a list of contributors to the report. (MDM)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

United States General Accounting Office

GAO

Report to the Secretary of Education

June 1995

ED 384 307

FEDERAL FAMILY EDUCATION LOAN INFORMATION SYSTEM

Weak Computer Controls Increase Risk of Unauthorized Access to Sensitive Data

HE028420

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

☑ This document has been reproduced as received from the person or organization originating it.

☐ Minor changes have been made to improve reproduction quality.

• Points of view or opinions stated in this document do not necessarily represent official OERI position or policy.

BEST COPY AVAILABLE

GAO/AIMD-95-117

2

GAO

United States
General Accounting Office
Washington, D.C. 20548

Accounting and Information
Management Division

B-260066

June 12, 1995

The Honorable Richard W. Riley
The Secretary of Education

Dear Mr. Secretary:

This report discusses weaknesses we identified during our assessment of the general controls over the Federal Family Education Loan Program (FFELP) information system maintained and operated by a contractor for the Department of Education. Such controls are critical to Education's ability to safeguard assets, maintain sensitive loan data, and ensure the reliability of financial management information.

The FFELP information system's general controls affect the system's overall effectiveness and the security of computer operations as opposed to being unique to any specific computer application. They include the organizational structure, operating procedures, software security features, and physical protection designed to ensure that access to data is appropriately restricted, only authorized changes are made to computer programs, computer security duties are segregated, and back-up and recovery plans are adequate to ensure the continuity of essential operations.

Education is required by 31 U.S.C. 3515 and 3521 to develop FFELP financial statements and have them audited. We audited FFELP's fiscal year 1992 financial statements, and we and Education's Office of the Inspector General (OIG) jointly audited the fiscal year 1993 financial statements. The OIG is auditing FFELP's fiscal year 1994 financial statements.

Our audit of FFELP's fiscal year 1993 financial statements disclosed that the FFELP information system's general control problems contributed to material weaknesses in internal controls affecting the accuracy of financial reports.[1] The system's general control problems warranted further examination and Education's prompt attention.

Results in Brief

Education's general controls over the FFELP information system did not adequately protect sensitive data files, applications programs, and systems software from unauthorized access, change, or disclosure. Education, for

[1]Financial Audit: Federal Family Education Loan Program's Financial Statements for Fiscal Years 1993 and 1992 (GAO/AIMD-94-131, June 30, 1994).

example, did not (1) adequately monitor the access activities of system users with special privileges that allow them to independently change the system or (2) record and report and, thus, could not review, successful access to sensitive computer data and programs. Further, outside users could potentially bypass the system's access controls to gain access to the system.

We reported FFELP information system general control problems in our audit of the program's fiscal year 1993 financial statements, and Education has made improvements. The improvements have resulted in Education and its contractor having appropriately segregated computer system duties and adequately prepared and tested disaster recovery plans. However, significant weaknesses continue in controlling system access and systems software changes.

The FFELP information system's serious access and systems software change control deficiencies resulted primarily from Education's overall weak computer security administration. Education did not adequately oversee the FFELP information system's computer security, which contributed to this problem. Further, Education had not developed, and its contractor had not implemented, adequate policies and procedures in key control areas.

Background

FFELP, formerly known as the Guaranteed Student Loan Program, primarily increases postsecondary education opportunities for eligible students who otherwise may not be able to further their education. The Department of Education relies extensively on schools, lenders, and guaranty agencies in making resources available to eligible students and overseeing the program. As of September 30, 1994, Education reported $77 billion in outstanding FFELP loan guarantees.

The FFELP information system supports the necessary functions to administer the guaranteed student loan program, analyze program activities, facilitate collection of defaulted guaranteed loans assigned to Education, and report financial information. Prior to October 1992, National Computer Systems in Iowa City, Iowa, operated and maintained the FFELP information system under contract with Education. Since then, another contractor, E-Systems, has provided the system's computer operation, data management, system programming, database administration, and security administration at E-Systems' computer facility in Greenville, Texas.

E-Systems also provides applications program development and maintenance support through a subcontractor in Arlington, Virginia. The subcontractor provides quality assurance support to ensure that all program development and modification efforts meet Education's programming, testing, and documentation standards.

Education's Program Systems Service Director is responsible for (1) establishing FFELP information system computer processing requirements and security guidance for the contractor, (2) approving all requests for computer access to the system, (3) initiating and approving all system enhancements and any program development efforts, (4) accepting new computer programs and modifications, and (5) monitoring the system's computer processing, controls, and disaster recovery activities. Responsibility for disaster recovery is shared by Education and E-Systems, which have a contract for off-site computer processing support in the event of a disruption to the Greenville computer operation.

The FFELP information system is composed of several separate systems, including the following.

- The Lender and School System. This system encompasses all processing associated with schools and lenders participating in the guaranteed student loan program. For example, it controls and accounts for payments to about 8,000 lenders for interest subsidies and special allowances, net of loan origination fees, which in fiscal year 1994 amounted to about $1.2 billion.
- The Guaranty Agency System. This system (1) controls payments to more than 40 guaranty agencies for losses on guaranteed student loans, which in fiscal year 1994 amounted to about $1.2 billion net of collections, (2) processes information reported by guaranty agencies on the condition of their guarantee and default portfolios, and (3) maintains data on individual guaranteed loan borrowers used to calculate default rates for over 7,500 participating schools.
- The Debt Management and Collections System. This system processes defaulted loan data from the time a debt is assigned to Education until it is paid in full or otherwise satisfied. The system (1) maintains account records, produces debtor letters and bills, and provides information to collectors attempting to collect on the accounts, (2) functions as an accounting system to track interest accruals, adjust account balances, record receipt of payments, and assess fees and charges, and (3) tracks information involved with accounts assigned to the Internal Revenue Service for tax refund offsets, collection agencies, and credit bureaus. As

of September 30, 1994, this system maintained information on more than 2.8 million FFELP loans valued at over $7.3 billion and on which about $458 million was collected during fiscal year 1994.

- The Support System. This system accounts for and controls financial transactions, provides various management and quality control reports, and provides control over and information regarding data used by the other systems and subsystems. For instance, this system has a financial information subsystem to summarize all FFELP financial transactions, such as payments, receivables, collections, write-offs, and cancellations, and to report them to Education's general ledger system.

In our fiscal year 1993 audit report, we reported that Education did not have effective general controls over the FFELP information system. Specifically, we found that (1) controls over access to data and computer programs were ineffective, (2) system software change controls were inadequate, (3) computer disaster recovery plan testing and evaluation procedures needed improvement, and (4) computer security administration, such as monitoring the contractor's system security operations, needed strengthening.

In February 1995, we reported to the Congress on the government's high-risk areas, including student financial aid.[2] In that report, we pointed out deficiencies in FFELP's financial statements disclosed by our audits under the Chief Financial Officers Act of 1990 (Public Law 101-576). We reported also that Education was taking corrective actions to, for example, address the need to improve controls over information and financial management systems to maintain the privacy of sensitive student loan data.

Objective, Scope, and Methodology

Our objective was to evaluate and test the effectiveness of general controls over the FFELP information system. Specifically, we evaluated controls to

- protect data and applications programs from unauthorized access;
- prevent unauthorized changes to systems software;
- provide segregation of duties involving applications and system programmers and of responsibilities for computer operations, security, and quality assurance;
- ensure recovery of computer processing operations in case of a disaster or other unexpected interruption; and

[2]High-Risk Series: Student Financial Aid (GAO/HR-95-10, February 1995).

- ensure adequate computer security administration.

To evaluate these controls, we identified and reviewed the FFELP information system's general control policies and procedures. Through discussions with Education and contractor staffs, including programming and operation personnel, we determined how the general controls should work and the extent to which they were considered by Education to be in place. We reviewed the installation and implementation of the contractor's system and security software.

We also identified and evaluated improvements over general controls made since the audit of Education's fiscal year 1993 financial statements. In addition, we discussed with Education staff the policies and procedures for overseeing its FFELP information system contractor computer security.

Further, we tested and observed the operation of general controls over the FFELP information system to determine whether they were in place, adequately designed, and operating effectively. We attempted, for example, to access sensitive data and programs. These attempts were performed with the knowledge and cooperation of Education and its contractor.

To assist in our evaluation and testing of general controls, we contracted with the public accounting firm of Ernst & Young. We determined the scope of our contractor's audit work, monitored its progress, and reviewed the related work papers to ensure that the resulting findings were adequately supported.

We performed our work at Education's headquarters in Washington, D.C., and at the contractor's computer processing installation in Greenville, Texas, and its subcontractor's system design and maintenance facility in Arlington, Virginia. Our review was performed from December 1994 through February 1995 in accordance with generally accepted government auditing standards.

We discussed our findings and Education's proposed corrective actions with Education and contractor officials. Education provided written comments on a draft of this report, which are included as appendix I.

Inadequate Controls Over Access to Data, Programs, and Software

A primary objective of a computer system's general controls is to safeguard data, protect computer applications programs, and prevent systems software from unauthorized access. Without effective access controls, the integrity and reliability of a computer system's data cannot be maintained, sensitive data can be accessed and changed, and information can be inappropriately disclosed.

The FFELP information system had serious computer security weaknesses that afforded opportunities for unauthorized access to the system's data, applications programs, and systems software. Also, access to sensitive system files and utility programs was not monitored because access was not recorded and reported. As a result, (1) the FFELP information system is vulnerable to unauthorized entry, (2) Education risks the inadvertent or deliberate misuse, fraudulent use, alteration, or destruction of important FFELP data, and (3) unauthorized access can occur without detection.

Access Was Not Controlled

Access controls over the FFELP's information system were not adequate to effectively protect loan data files, computer applications programs, and systems software from unauthorized use. Unauthorized access could ultimately affect the integrity of sensitive student loan data and the reliability of financial management information.

Our review showed that unauthorized personnel could bypass normal, existing security controls, and that controls were not in place to prevent outside system users from gaining access to the FFELP's information system. Our observations and testing disclosed the following weaknesses.

- Any of Education's 139 staff who had authorized computer access could also gain access to the private user libraries of the two Education staff responsible for FFELP information system security administration tasks. Entry to these libraries could assist in further penetrating the system's access controls. Therefore, people authorized to use the system had the means to indiscriminately and improperly read, alter, or delete data, and then delete all evidence of a system compromise.
- Because the contractor's computer network allowed unrestricted batch access,[3] entry to the FFELP information system could be made through other systems operated by the contractor. In addition to the FFELP information system, the system's contractor also operates computer systems for other government entities and private sector companies. As a

[3]In computer operations, batch access is the processing of a group of related transactions or other items at periodic intervals.

result, an indeterminable number of non-Education users who had access to the contractor's other systems could have gained entry to the FFELP information system by submitting batch jobs through the contractor's other systems. (As discussed later, Education advised us that, subsequent to our review, the contractor corrected this problem.)

- The system allowed users to gain unauthorized access to several sensitive systems utility programs used to maintain the system's computer and assist in its operations. Once accessed, these utility programs could be used to modify systems data and to bypass access controls.
- There were no controls in place to prevent unrestricted access to several sensitive systems software files. These files contain important access control information, such as users' identifications and passwords. With this information, an unauthorized person could access and obtain sensitive information in guaranty agency records, lender information, and delinquent debtor files. Such access could result in the alteration of records affecting monetary transactions.

In addition, we found that special access privileges were granted to 10 contractor personnel allowing them to independently insert, modify, or delete virtually any student loan data or related computer application programs and systems software. Special access privileges are appropriate for limited purposes, such as to handle problems or emergencies that interrupt the system's 24-hour-a-day operation. However, controls were not in place to monitor the access activities of those with special access privileges, resulting in the possibility that unauthorized changes could be made and not be detected. In addition, there was no assurance that the special privileges were being appropriately used or were needed. When we previously reported this situation to Education, it reduced from 17 to 7 the number of people having these special access privileges, but controls to monitor these authorizations were still weak.

Further, we found that access to the FFELP information system was possible through special user identifications assigned to complete specific computer related tasks and used to gain emergency access. Because of their nature, special user identifications are not assigned to individuals. However, the special user identifications allow unlimited access to virtually all FFELP computer resources. Although 14 special user identifications were in use at the time of our review, none had been formally reviewed and approved by Education before being issued. Without Education's approval, there is no assurance that the access granted through the special user identifications is consistent with

established policies and that access is only given to information needed for required jobs.

For the areas in which we found poor access controls, Education lacked policies and procedures to protect the system's data, applications programs, and systems software. For example, Education did not have procedures regarding access to sensitive data, private computer user libraries, and utility programs. Also, the FFELP information system did not report successful access to sensitive files, which the next section discusses. These problems are also symptomatic of broader computer security administration weaknesses, discussed later in this report.

Education acknowledged the FFELP information system's serious access control weaknesses. Also, to address all of the access control weaknesses we identified, Education advised us that (1) since the completion of our review, the FFELP information system's contractor has made access control improvements and (2) Education plans, during fiscal year 1995, additional corrective actions to reduce the exposure access control problems create.

Education said that the contractor has, for example, implemented controls over access from other systems within the contractor's network by testing batch jobs for Education users' identifications and passwords and canceling batches without proper Education authorization. Also, Education's Director of Program Systems Service told us that the Department and its contractor plan, for instance, to (1) perform periodic reviews of sensitive data files to ensure that inappropriate changes are not made and (2) write procedures requiring sensitive utility programs to be removed from public access libraries and placed in a controlled library.

Access Reporting Is Incomplete

Although the FFELP information system reports violations involving unsuccessful attempts to access sensitive files and utility programs, the system does not record successful access. Because access reporting is incomplete, there is no means of detecting unauthorized changes to these files and programs by people who have gained authorized access. An effective access reporting system is central to maintaining the integrity of sensitive computer information and related systems software. This is a normal and effective computer security control technique and one which the FFELP information system is capable of providing.

Monitoring the access to the FFELP information system by authorized users, especially those who have the ability to alter sensitive files and programs

and those who have special access privileges, is necessary to help identify significant problems and deter these users from inappropriate and unauthorized activities. This control technique can be implemented by using the audit trail capability of the FFELP information systems software.

Using this capability would require Education to compile a list of sensitive system files and utility programs so that access to these resources are recorded and reported. Access reports would then be available to managers to highlight activity that is unusual or suspicious so that it can be investigated. This process would provide the active oversight necessary to help ensure that problems are deterred or detected by allowing managers to periodically review the appropriateness of successful systems access.

Education has recognized the necessity of establishing more complete access reporting procedures and plans to compile a list of sensitive system files and utility programs. Also, Education plans to selectively record access to these files and programs, including recording access made by authorized FFELP users with special access privileges.

Effectiveness of Other General Controls Varied

In addition to access controls, a computer system typically has other important general controls to ensure the integrity and reliability of data. These general controls include policies, procedures, and control techniques to (1) prevent unauthorized changes to system software, (2) provide segregation of duties involving applications and systems programmers and of responsibilities for computer operations, security, and quality assurance, and (3) ensure continuation of computer processing operations in case of an unexpected interruption.

Regarding these areas, our review showed that the FFELP information system's controls over systems software changes continue to be ineffective. However, the weaknesses we previously reported in the areas of segregation of duties and disaster recovery plans were corrected.

Unauthorized Systems Software Changes Not Prevented

A standard computer control practice is to ensure that only authorized and fully tested systems software is placed in operation. An effective systems software change control process would involve verifying that (1) systems software changes are documented and authorized and (2) changes are tested and independently reviewed to ensure that such changes work as intended and do not result in loss of data and program integrity.

Our review showed that the FFELP information system contractor's systems software change process was not working effectively. For example, Education's contractor could not locate systems software change authorization forms for five of eight randomly selected systems software changes made during calendar year 1994. Also, for one of these undocumented changes, we were told that only verbal approval had been given. A computer facility would usually maintain authorization documentation as a permanent record of valid and approved systems software changes.

Also, for the systems software changes we examined, we could not determine whether adequate testing had been conducted. Specifically, in four cases for which information on testing and related test plans was available, the documentation was unclear as to the extent and adequacy of testing. Further, we were unable to find evidence of an independent review or documentation relating to acceptance testing and verification for any of the systems software changes we examined.

To correct these and previously reported systems software change control inadequacies, during 1994, the FFELP information system's contractor established for the first time, a system software change control process. In December 1994, the contractor created a Change Control Board responsible for overseeing all systems software changes. However, at the time of our review, the procedures to improve control of systems software changes had not yet been completed or implemented. These procedures are necessary to ensure that systems software changes are properly authorized and consistently and completely documented.

Education officials told us that they plan to work more closely with the contractor to ensure that all systems software changes go through a formal change control process. Further, we were told that this process will include documentation of acceptance test activities and independent review by Education of test results.

Important Computer System Duties Appropriately Segregated

A fundamental control technique for an agency's computer operations commonly involves the appropriate segregation of duties and responsibilities of computer personnel. We previously advised Education of duties that were not appropriately separated. For instance, Education's security administrator was part of the systems software support group; thus, the security administrator lacked independence in overseeing the software support group's activities. In September 1994, the FFELP

information system's contractor established security administration as a separate function, which strengthened the separation of duties.

Overall, our review showed that these and other roles and responsibilities involving the FFELP information system were appropriate. Such functions as applications programming, computer operations, security, and systems programming were adequately established to ensure segregation of duties.

Disaster Recovery Plans Improved

Ordinarily, an agency must ensure that it is adequately prepared to cope with a potential loss of operational capability due to an earthquake, fire, accident, sabotage, or any other operational disruption. A reliable, current, and tested disaster recovery plan is essential to ensure that the FFELP information system can restore operations and data in the event of a disaster.

Previously, we reported that Education's disaster recovery plan and testing, and evaluation of test results, needed to be improved. Education corrected its disaster recovery plan weaknesses by (1) testing its emergency team notification process to ensure that team members know who to contact and their specific role in the event of a disaster and (2) identifying the objectives and expected results of a disaster recovery test for use in comparing and evaluating actual tests.

Computer Security Administration Remains Weak

The FFELP information system's general control problems persist primarily because Education has not developed and implemented a computer security administration program to ensure that the contractor maintained adequate general controls. While some corrective measures have been taken, FFELP information system general controls remain ineffective in several key areas. These shortcomings hamper effective systems security and weaken protection of the system's data resources.

While a contractor operates and maintains the FFELP information system, Education is responsible for establishing appropriate computer security policies and procedures and overseeing the contractor's compliance with them. Nonetheless, our reviews of the FFELP information system's general controls during audits of the program's financial statements for the past 3 fiscal years have shown that Education does not effectively manage or monitor the contractor's computer security operations.

We reported last year, for example, that Education and its contractor had taken or planned corrective actions to develop a system to monitor activities of personnel with broad-based or privileged access to FFELP data. This year, we noted that such corrective actions were not yet implemented.

Moreover, in September 1993, we advised Education that the FFELP information system's computer security administration needed strengthening. In response, officials proposed establishing a security oversight staff responsible for security controls over the FFELP information system. However, this proposal was not implemented.

Since then, Education updated its guidance to the FFELP information system's contractor and users on security policies and procedures. However, these current policies and procedures still do not

- address standards for classifying and protecting sensitive financial data, systems software, and applications programs;
- identify standard security software options to be used in implementing security software over Education's files and programs;
- require that computer access accounts be established based on standard job functions; and
- prescribe procedures to monitor authorized users' activities and to follow up on security violations and enforce Education's guidance.

Also, in September 1993, we advised Education that its security administrator position, which had been vacant for a month, needed to be promptly filled. The security administrator has a key role in coordinating day-to-day functions of the security software administration. Although Education agreed to hire a security administrator on a priority basis, the position was vacant for another 13 months—until September 1994.

These delays, unresolved problems, and incomplete instructions are indications of Education's failure to give adequate priority to the effective implementation and oversight of general controls for the FFELP information system. Education can bolster its attention to the FFELP information system's security administration by developing and implementing a computer security administration program.

A security administration program would include

- a broad institutional policy statement on information security;

- clearly defined roles and responsibilities of employees, information owners, user departments, regional security administrators, and Education's and the contractor's security officers; and
- explicitly assigned responsibility for administering security policies and procedures.

To ensure that the FFELP information system's security oversight is complete, this program would need to be integrated with the contractor's own security plans.

A computer security administration program would provide Education the solid basis necessary to effectively monitor the contractor's operations to ensure that an adequate security environment is maintained. Also, stronger oversight through a computer security administration program would help to minimize the serious risk of unauthorized access to FFELP information system data caused by the computer security weaknesses we found.

In February 1995, Education officials agreed to enhance the FFELP information system's security administration during fiscal year 1995. Also, we were told that Education's Program Systems Service will assign an individual to provide security oversight.

Conclusions

Sound general controls, especially computer access and system software change controls, are critical to Education's ability to maintain the confidentiality of sensitive student loan data and ensure the reliability of financial management information. While the FFELP information system's general controls have improved in some respects, the system remains vulnerable because of inadequate access restrictions, incomplete information for monitoring authorized users' activities, and weak systems software change controls.

A computer security administration program to manage and monitor the FFELP information system's computer security operations would assist Education in giving priority attention to resolving these persistent problems. Also, strengthening general controls and reducing the system's computer security risks will require Education to (1) develop and implement policies and procedures to restrict access to computer data, applications programs, and systems software, (2) report successful access to sensitive system files and programs, and (3) establish controls to prevent unauthorized changes to the systems software.

Recommendations

We recommend that you direct the Director of the Program Systems Service to

- develop and implement a computer security administration program to oversee the FFELP information system's computer security control operations;
- develop, and require the FFELP information system's contractor to implement, policies and procedures to limit access authorizations for the system's users to only those computer programs and data needed to perform their duties, and to approve the creation of special user identifications;
- identify sensitive data files and programs and monitor successful access to them, including access by users having special access privileges; and
- require the FFELP information system's contractor to devise controls to ensure that only approved and tested changes are made to the systems software.

Agency Comments and Our Evaluation

Education fully agreed with our recommendations to improve the FFELP information system general control environment. In his written comments on a draft of this report, the Senior Advisor to the Secretary said that the Office of Postsecondary Education's Program Systems Service has implemented new security oversight procedures and worked with the contractor to remedy access and software control problems.

The Senior Advisor said that these actions have included

- establishing a system security oversight team, appointing a security oversight team leader to oversee the implementation of security procedures, and providing guidance for the FFELP security program;
- requiring the contractor to place sensitive system data in a restricted library and sensitive utility programs in a controlled library, and establishing a formal process to control special user identifications;
- reemphasizing to the contractor that all system programming changes to the FFELP system software must be documented, tested, and approved before being implemented, and imposing sanctions for contractor noncompliance; and
- monitoring systems access by the systems programming staff through on-line access reports that are reviewed daily by security personnel.

The Senior Advisor said also that additional corrective actions were planned and in process. These included (1) drafting a broad information

policy statement on information security for the FFELP program that defines security roles and responsibilities for Education and contractor personnel, sets standards for protecting sensitive data, and requires computer access to be based on job function and (2) evaluating an off-the-shelf software audit product to detect unauthorized changes to the FFELP system and database.

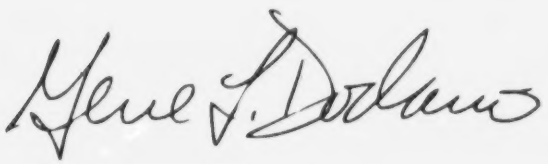
Education's actions are necessary to improve control over access to FFELP information system data, programs, and software. It is important for Education to complete its planned actions and to monitor the results of these and the actions already taken to verify that security vulnerabilities have been corrected. Education's top management's continued concern for resolving these issues is also critical to addressing FFELP information system security problems.

This report contains recommendations to you. The head of a federal agency is required by 31 U.S.C. 720 to submit a written statement on actions taken on these recommendations to the Senate Committee on Governmental Affairs and the House Committee on Government Reform and Oversight not later than 60 days after the date of this report and to the House and Senate Committee on Appropriations with the agency's first request for appropriations made more than 60 days after the date of this report.

We are sending copies of this report to the Chairmen and Ranking Minority Members of the Senate Committee on Governmental Affairs, the House Committee on Government Reform and Oversight, the Senate Committee on Labor and Human Resources, the House Committee on Economic and Educational Opportunities, and other interested congressional committees. Copies will be made available to others upon request.

This report was prepared under the direction of Lisa G. Jacobson, Director, Civil Audits, who can be reached at (202) 512-9508, if you or your staff have any questions. Other major contributors to this report are listed in appendix II.

Sincerely yours,



Gene L. Dodaro
Assistant Comptroller General

Contents

Letter	1
Appendix I Comments From the Department of Education	20
Appendix II Major Contributors to This Report	24

Abbreviations

FFELP	Federal Family Education Loan Program
OIG	Office of the Inspector General

Comments From the Department of Education

UNITED STATES DEPARTMENT OF EDUCATION
WASHINGTON, D.C. 20202-_____

MAY 18 1995

Mr. Gene L. Dodaro
Assistant Comptroller General
Accounting and Information Management Division
U.S. General Accounting Office
Washington, D.C. 20548

Dear Mr. Dodaro:

This responds to your April 26, 1995 request for comments on the General Accounting Office (GAO) draft audit report entitled "Federal Family Education Loan Information System: Weak Computer Controls Increase Risk of Unauthorized Access to Sensitive Data" (GAO/AIMD-95-117). We appreciate the opportunity to review and comment on the draft report on the general controls over the Federal Family Education Loan Program (FFELP) information system.

As noted in your draft report, since GAO's audit of the Fiscal Year 1993 FFELP Financial Statements, the Department has improved the general controls pertaining to segregation of duties and disaster recovery contingency planning. We are in full agreement with the additional recommendations made in this report to improve the FFELP information system general control environment.

Most of the issues mentioned in the draft report deal with computer access and system software change controls for sensitive systems. Since the completion of your review, the Office of Postsecondary Education's Program Systems Service (PSS) implemented new security oversight procedures and worked with the contractor to remedy access and software control problems. Also, during Fiscal Year 1995, PSS plans additional corrective actions to reduce the potential exposure. We believe that these measures and ongoing initiatives will address the concerns raised in the audit report. Our completed and proposed corrective actions to the recommendations included in the draft audit report follow.

Corrective actions implemented

- To improve communication on security issues, PSS established a systems security oversight team and appointed a security oversight team leader to oversee the implementation of security procedures prescribed by the Office of Postsecondary Education's Computer Security Officer.

- To prevent unauthorized and inappropriate access by other system users within the contractor's network, the contractor was required to place sensitive system datasets in a restricted library and sensitive utility programs in a controlled library. In addition, a formal process was established to control special user identifications

Our mission is to ensure equal access to education and to promote educational excellence throughout the Nation

- To ensure that only approved and tested changes are made to the system software, PSS reemphasized to the contractor that all system programming changes to the FFELP system software must be documented, tested, and approved before being implemented. In addition, contractor oversight for existing configuration management polices and procedures will be provided via the Configuration Control Board that meets weekly. Sanctions will be imposed for contract non-compliance.

- To monitor and review the FFELP system access by systems programming staff, additional security procedures were implemented.

Corrective actions in-process

- To implement the computer security administration program, PSS is drafting a broad information policy statement on information security for the FFEL Program that defines security roles and responsibilities for Education and contract personnel, sets standards for protecting sensitive data, and requires computer access to be based on job function.

- To enhance the Department's ability to monitor and review FFELP system access by programming staff, PSS is evaluating an off-the-shelf software audit product to detect unauthorized changes to the FFELP system and database.

Enclosed are our detailed responses to the specific recommendations included in the draft audit report. If you have any questions on these corrective actions, please feel free to contact Carl O'Riley, Director of Program Systems Service at (202) 708-7701.

Yours sincerely,

Leo Kornfeld
Senior Advisor to the Secretary

Enclosure

cc: David Longanecker, Assistant Secretary for Postsecondary Education
Don Wurtz, Chief Financial Officer

Enclosure

DETAILED RESPONSES TO THE DRAFT REPORT RECOMMENDATIONS
(GAO/AIMD-95-117)

The Director of the Program Systems Service should:

Recommendation 1. *Develop and implement a computer security administration program to oversee the FFELP information system's computer security control operations.*

Response: We concur. On May 1, 1995, the Director of the Program Systems Service (PSS) established a Security Oversight Team and appointed a PSS Security Oversight Team Leader. The overall mission of the Security Oversight Team is to ensure: (1) each system administered by the PSS complies with all applicable security requirements of the Department and OPE's Security Officer; (2) employees are trained in security matters; and, (3) security procedures are documented for each system.

Concurrently, on May 1, 1995, the PSS Director established a three member FFELP Security Team headed by a FFELP Security Officer--who is also a member of the Security Oversight Team. Each FFELP Security Team member is assigned specific security duties.

On April 19, 1995, the PSS drafted a security policy statement entitled, "Federal Family Education Loan Program Information Security Policy." The purpose of this document is to provide broad institutional policy for FFELP information security by: (1) defining security roles and responsibilities both for Departmental and contract employees; (2) identifying the standards for classifying and protecting sensitive data; and (3) requiring computer access to be based on job function. Enhancements to the draft policy statement are to be provided by the Security Oversight Team. The final version is expected to be ready for implementation in Fiscal Year 1995.

Recommendation 2. *Develop and require the FFELP information system's contractor to implement policies and procedures to limit access authorizations for the system's users to only those computer programs and data needed to perform their duties, and to approve the creation of special user identifications.*

Response: We concur. On April 1, 1995, PSS required the FFELP contractor to remove sensitive system datasets from the Global Access Table and to place these datasets in a restricted library. PSS will perform periodic reviews to ensure that inappropriate changes are not made to the datasets. Concurrently, the FFELP contractor was required to move sensitive utility programs from public libraries to a controlled library. Both actions should prevent unauthorized and inappropriate access by other systems users within the contractor's network. In addition, the Department now formally approves the creation of special user identifications. This procedure was implemented in 1994.

Recommendation 3. *Identify sensitive data files and programs and monitor successful access to them, including access by users having special access privileges.*

Response: We concur. In April 1995, PSS activated the audit function in the FFELP RACF program to monitor and review systems access by the systems programming staff. On-line access reports are reviewed daily by security personnel. One third of the systems programming staff will be reselected--by random sample--for audit every three months or as required.

Additionally, to enhance PSS' ability to monitor and review access to the FFELP information system IDMS Relational Database Management System (RDMS), the Department is currently evaluating a new off-the-shelf software audit product (TRACER) on a 30 day trial basis. TRACER is expected to provide before and after images of user changes to database fields. This ability should allow selected users to be successfully monitored by PSS security personnel. If the trial test is successful, TRACER will be added to the FFELP system software. If not, the Department will continue to look for an effective RDMS audit tool during Fiscal Year 1995.

Recommendation 4. *Require the FFELP information system's contractor to devise controls to ensure that only approved and tested changes are made to the systems software.*

Response: We concur. In 1994, PSS instructed the FFELP information system's contractor to follow existing procedures for the migration of new systems software products and changes to existing systems software to the FFELP production environment. Also, the PSS Director reiterated this requirement in an April 1995 follow up meeting with the contractor's Vice President. In addition, contractor oversight for existing configuration management policies and procedures is provided via the Configuration Control Board that meets on a weekly basis. The contractor will be instructed in writing to adhere to existing configuration management policies and procedures. If the contractor does not adhere to the existing policies and procedures, appropriate action will be taken.

Major Contributors to This Report

Accounting and Information Management Division, Washington, D.C.	Robert Dacey, Senior Assistant Director Crawford Thompson, Assistant Director
Resources, Community, and Economic Development Division, Washington, D.C.	Barbara Johnson, Senior Auditor
Dallas Regional Office	David W. Irvin, Senior Auditor

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 6015
Gaithersburg, MD 20884-6015

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (301) 258-4066, or TDD (301) 413-0006.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (301) 258-4097 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

BEST COPY AVAILABLE

PRINTED ON RECYCLED PAPER

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Correction Requested

SHIP TO:
GAIL MATHEWS
1301 PICCARD DR. S-300
ROCKVILLE MD 20850

Request # 3428813 19 3
m
06/19/95 / 14:32 v
06/19/95 / 21:04

3428813011p205
Item Document Number
1 AIMD-95-117

BEST COPY AVAILABLE